IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDA COOPER, CORAL FRASER, DAVID GILTIN, and GILBERT MANDA, *on behalf of themselves and all others similarly situated,* Plaintiffs, v. MOUNT SINAI HEALTH SYSTEM, INC., Defendant.	No. 1:23-cv-09483 (PAE) Hon. Paul A. Engelmayer

~~[PROPOSED]~~ STIPULATED CONFIDENTIALITY AGREEMENT

The parties to this Stipulated Confidentiality Agreement have agreed to the terms of this Order; accordingly, it is **ORDERED**:

1. **Scope.** All materials produced or adduced in the course of discovery—including, but not necessarily limited to, initial disclosures, information derived from subpoenas, responses to discovery requests, deposition testimony and exhibits, and information derived directly therefrom (collectively referred to herein as "Documents")—shall be subject to this Order concerning Confidential Information as defined below. This Order is subject to the Local Rules of this District and the Federal Rules of Civil Procedure on matters of procedure and calculation of time periods.

2. **Confidential Information.** As used in this Order, "Confidential Information" means information designated as "CONFIDENTIAL-SUBJECT TO CONFIDENTIALITY AGREEMENT" by the Designating Party (as defined below) that falls within one or more of the following categories:

a. information prohibited from transfer or disclosure by statute, including but not limited to the Healthcare Insurance Portability and Accountability Act of 1996 ("HIPAA"), 42 U.S.C. §§ 1320d, *et seq.* and the regulations issued by the Department of Health and Human Services under HIPAA;

b. information that reveals trade secrets or confidential or proprietary financial information that the Designating Party has maintained as confidential or is required by agreement to be maintained as confidential;

c. confidential medical information, personal identity information, and personally identifiable information concerning any individual;

d. income tax returns (including attached schedules and forms), W-2 forms, and 1099 forms; and

e. personnel or employment records of a person who is not a party to the case.

3. **Designating Party.** As used in this Order, "Designating Party" means any person (including third parties) that produces Documents or provides information for use in this Action during the course of this litigation ("Producing Party") and invokes the terms of this Order by designating information or Documents pursuant to Paragraphs 4 and 6 below.

4. **Designation.**

a. A party shall designate a Document as Confidential Information for protection under this Order only the Documents listed in Paragraph 2 above, by placing or affixing the words "CONFIDENTIAL - SUBJECT TO CONFIDENTIALITY AGREEMENT" on the pages of the Document containing Confidential Information and on each page of all copies containing Confidential Information in a manner that will not interfere with the legibility of the Document. As used in this

Order, "copies" includes electronic images, duplicates, summaries or descriptions that contain Confidential Information.

b. Where a Document includes both Confidential Information and non-Confidential Information, only those portions of the Document which contain Confidential Information may be designated as such.

c. The marking "CONFIDENTIAL - SUBJECT TO CONFIDENTIALITY AGREEMENT" shall be applied prior to or at the time the Documents are produced or disclosed. Applying the marking "CONFIDENTIAL - SUBJECT TO CONFIDENTIALITY AGREEMENT" to a Document does not mean that the Document has any status or protection by statute or otherwise except to the extent and for the purposes of this Order.

d. Any copies that are made of any Documents marked "CONFIDENTIAL - SUBJECT TO CONFIDENTIALITY AGREEMENT" shall also be so marked, except that indices, electronic databases, or lists of Documents that do not contain substantial portions or images of the text of marked Documents and do not otherwise disclose the substance of the Confidential Information are not required to be marked.

e. The designation of a Document as Confidential Information is a certification by an attorney that the Document contains Confidential Information as defined in this order.

5. **Depositions.** Unless all parties agree on the record at the time the deposition testimony is taken, all deposition testimony taken in this case shall be treated as Confidential Information until the expiration of the following: No later than the fourteenth day after the

transcript is delivered to any party or the witness, and in no event later than 60 days after the testimony was given. Within this time period, a party may serve a Notice of Designation to all parties of record as to specific portions of the testimony that are designated Confidential Information, and thereafter, only those portions identified in the Notice of Designation shall be protected by the terms of this Order. The failure to serve a timely Notice of Designation shall waive any designation of testimony taken in that deposition as Confidential Information, unless otherwise ordered by the Court or otherwise agreed upon by the parties.

6. **Protection of Confidential Material.**

   a. **General Protections.** Confidential Information shall not be used or disclosed by the parties, counsel for the parties, or any other persons identified in Subparagraph (b) for any purpose whatsoever other than in this litigation, including any appeal thereof. Because this is a putative class action, Confidential Information may be disclosed only to the named plaintiff(s) and not to any other member of the putative class unless and until a class including the putative member has been certified.

   b. **Limited Third-Party Disclosures.** The parties and counsel for the parties shall not disclose or permit the disclosure of any Confidential Information to any third person or entity except as set forth in Subparagraphs (i)-(ix). Subject to these requirements, the following categories of persons may be allowed to review Confidential Information:

      i. **Counsel.** Counsel for the parties and employees of counsel who have responsibility for the action including, but not limited to, contract attorneys hired for review purposes;

ii. **Parties.** Individual parties and employees and contractors of a party but only to the extent counsel determines in good faith that the employee's assistance is reasonably necessary to the conduct of the litigation in which the information is disclosed;

iii. **The Court and its personnel;**

iv. **Court Reporters and Recorders.** Court reporters and recorders engaged for depositions;

v. **Contractors.** Those persons specifically engaged for the limited purpose of making copies of documents or organizing or processing documents, including outside vendors hired to process electronically stored documents;

vi. **Consultants and Experts.** Consultants, investigators, or experts employed by the parties or counsel for the parties to assist in the preparation and trial of this action but only after such persons have completed the certification contained in Attachment A, Acknowledgment of Understanding and Agreement to Be Bound;

vii. **Witnesses at depositions.** During or in preparation for their depositions or testimony at trial or any hearing, witnesses (actual or potential) in this action to whom disclosure is reasonably necessary. Witnesses shall not retain a copy of documents containing Confidential Information, except witnesses may receive a copy of all exhibits marked at their depositions in connection with review of the transcripts. Pages of transcribed deposition testimony or exhibits to depositions that are designated as Confidential Information pursuant to the process set out in this Order must be separately bound by

the court reporter and may not be disclosed to anyone except as permitted under this Order.

viii. **Author or recipient.** The author or recipient of the document (not including a person who received the document in the course of litigation); and

ix. **Others by Consent.** Other persons only by written consent of the Producing Party or upon order of the Court and on such conditions as may be agreed or ordered.

c. **Control of Documents.** Counsel for the parties shall make reasonable efforts to prevent unauthorized or inadvertent disclosure of Confidential Information. Counsel shall maintain the originals of the forms signed by persons acknowledging their obligations under this Order for a period of three years after the termination of the case.

7. **Inadvertent Failure to Designate.** An inadvertent failure to designate a document as Confidential Information does not, standing alone, waive the right to so designate the document; provided, however, that a failure to serve a timely Notice of Designation of deposition testimony as required by this Order, even if inadvertent, waives any protection for deposition testimony. If a party designates a document as Confidential Information after it was initially produced, the receiving party, on notification of the designation, must make a reasonable effort to assure that the document is treated in accordance with the provisions of this Order. No party shall be found to have violated this Order for failing to maintain the confidentiality of material during a time when that material has not been designated Confidential Information, even where the failure to so designate was inadvertent and where the material is subsequently designated Confidential Information.

8. **Filing of Confidential Information.** This Order does not, by itself, authorize the filing of any document or any part thereof under seal. Rather, any documents intended by any party to be filed under seal must be noticed for hearing prior to the due date of the particular filing, showing good cause for sealing a portion of the record in the case. The mere fact that information has been designated as confidential by a party is insufficient to permit under-seal filing. A party seeking to file material under seal must set forth in its motion the reasons why the record should be sealed.

9. **No Greater Protection of Specific Documents.** Except on privilege grounds not addressed by this Order, no party may withhold information from discovery on the ground that it requires protection greater than that afforded by this Order unless the party moves for an order providing such special protection.

10. **Challenges by a Party to Designation as Confidential Information.** The designation of any material or Document as Confidential Information is subject to challenge by any party. The following procedure shall apply to any such challenge.

    a. **Meet and Confer.** A party challenging the designation of Confidential Information must do so in good faith and must begin the process by conferring directly with counsel for the Designating Party. In conferring, the challenging party must explain the basis for its belief that the confidentiality designation was not proper and must give the Designating Party an opportunity to review the designated material, to reconsider the designation, and, if no change in designation is offered, to explain the basis for the designation. The Designating Party must respond to the challenge within five (5) business days.

b. **Judicial Intervention.** A party that elects to challenge a confidentiality designation may file and serve a motion that identifies the challenged material and sets forth in detail the basis for the challenge. Each such motion must be accompanied by a competent declaration that affirms that the movant has complied with the meet and confer requirements of this procedure. The burden of persuasion in any such challenge proceeding shall be on the Designating Party. Until the Court rules on the challenge, all parties shall continue to treat the materials as Confidential Information under the terms of this Order.

11. **Action by the Court.** Applications to the Court for an order relating to materials or Documents designated Confidential Information shall be by motion. Nothing in this Order or any action or agreement of a party under this Order limits the Court's power to make orders concerning the disclosure of Documents produced in discovery or at trial.

12. **Use of Confidential Documents or Information at Trial.** Nothing in this Order shall be construed to affect the use of any Document, material, or information at any trial or hearing. A party that intends to present or that anticipates that another party may present Confidential Information at a hearing or trial shall bring that issue to the Court's and parties' attention by motion or in a pretrial memorandum without disclosing the Confidential Information. The Court may thereafter make such orders as are necessary to govern the use of such Documents or information at trial.

13. **Confidential Information Subpoenaed or Ordered Produced in Other Litigation.**

a. If a receiving party is served with a subpoena or an order issued in other litigation that would compel disclosure of any material or Document designated in this action as Confidential Information, the receiving party must so notify the Designating

Party, in writing, immediately and in no event more than seven (7) court days after receiving the subpoena or order. Such notification must include a copy of the subpoena or court order.

b. The receiving party also must immediately inform in writing the party who caused the subpoena or order to issue in the other litigation that some or all of the material covered by the subpoena or order is the subject of this Order. In addition, the receiving party must deliver a copy of this Order promptly to the party in the other action that caused the subpoena to issue.

c. The purpose of imposing these duties is to alert the interested persons to the existence of this Order and to afford the Designating Party in this case an opportunity to try to protect its Confidential Information in the court from which the subpoena or order issued. The Designating Party shall bear the burden and the expense of seeking protection in that court of its Confidential Information, and nothing in these provisions should be construed as authorizing or encouraging a receiving party in this action to disobey a lawful directive from another court. The obligations set forth in this paragraph remain in effect while the party has in its possession, custody, or control Confidential Information by the other party to this case.

14. Challenges by Members of the Public to Sealing Orders. A party or interested member of the public has a right to challenge the sealing of particular documents that have been filed under seal, and the party asserting confidentiality will have the burden of demonstrating the propriety of filing under seal.

15. Obligations on Conclusion of Litigation.

a. **Order Continues in Force.** Unless otherwise agreed or ordered, this Order shall remain in force after dismissal or entry of final judgment not subject to further appeal.

b. **Disposition of Confidential Information and Documents.** Within sixty (60) days after dismissal or entry of final judgment not subject to further appeal, all Confidential Information and Documents marked "CONFIDENTIAL - SUBJECT TO CONFIDENTIALITY AGREEMENT" under this Order, including copies as defined in ¶ 3(a), shall be returned to the Producing Party upon written request within ten (10) business days unless: (1) the Document has been offered into evidence or filed without restriction as to disclosure; (2) the parties agree to destruction to the extent practicable in lieu of return; or (3) as to Documents bearing the notations, summations, or other mental impressions of the receiving party, that party elects to destroy the Documents and certifies to the Producing Party that it has done so.

c. **Retention of Work Product and one set of Filed Documents.** Notwithstanding the above requirements to return or destroy Documents, counsel may retain (1) attorney work product, including an index that refers or relates to designated Confidential Information so long as that work product does not duplicate verbatim substantial portions of Confidential Information, and (2) one complete set of all Documents filed with the Court including those filed under seal. Any retained Confidential Information shall continue to be protected under this Order. An

attorney may use his or her work product in subsequent litigation, provided that its use does not disclose or use Confidential Information.

d. **Deletion of Documents filed under Seal from Electronic Case Filing (ECF) System.** Filings under seal shall be deleted from the ECF system only upon order of the Court.

16. **Order Subject to Modification.** This Order shall be subject to modification by the Court on its own initiative or on motion of a party or any other person with standing concerning the subject matter.

17. **No Prior Judicial Determination.** This Order is entered based on the representations and agreements of the parties and for the purpose of facilitating discovery. Nothing herein shall be construed or presented as a judicial determination that any document or material designated Confidential Information by counsel or the parties is entitled to protection under Rule 26(c) of the Federal Rules of Civil Procedure or otherwise until such time as the Court may rule on a specific document or issue.

18. **HIPAA Qualified Protective Order**. It is the intent of the parties that this Order be deemed a "qualified protective order" under HIPAA, as set forth in the implementing regulations for that statute found at 45 C.F.R § 164.512(e).

19. **Persons Bound.** This Order shall take effect when entered and shall be binding upon all counsel of record and their law firms, the parties, and persons made subject to this Order by its terms.

IT IS SO STIPULATED, through Counsel of Record, this 6th day of December 2024.

/s/ David A. Carney
David A. Carney (*pro hac vice*)
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, OH 44114
(216) 861-7634
dcarney@bakerlaw.com

/s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
(202 558-5500
jbilsborrow@weitzlux.com

/s/ Robyn M. Feldstein
Robyn M. Feldstein
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
(212) 589-4201
rfeldstein@bakerlaw.com

Counsel for Defendant
Mount Sinai Health System, Inc.

/s/ David S. Almeida
David S. Almeida
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, IL 60614
(312) 576-3024
david@almeidalawgroup.com

Counsel for Plaintiffs
& the Proposed Class

SO ORDERED:

Dated: December 10, 2024

Paul A. Engelmayer
Judge Paul A. Engelmayer

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDA COOPER, CORAL FRASER, DAVID GILTIN and GILBERT MANDA, *on behalf of themselves and all others similarly situated,* Plaintiffs, v. MOUNT SINAI HEALTH SYSTEM, INC., Defendant.	No. 1:23-cv-09483 (PAE) Hon. Paul A. Engelmayer

ACKNOWLEDGMENT OF UNDERSTANDING AND AGREEMENT TO BE BOUND

The undersigned hereby acknowledges that they have read the Stipulated Confidentiality Agreement entered into in the above-captioned action and attached hereto, understands the terms thereof, and agrees to be bound by its terms. The undersigned submits to the jurisdiction of the United States District Court for the Southern District of New York in matters relating to the Stipulated Confidentiality Agreement and understands that the terms of the Stipulated Confidentiality Agreement obligate the undersigned to use materials designated as Confidential Information in accordance with the Order solely for the purposes of the above-captioned action, and not to disclose any such Confidential Information to any other person, firm or concern.

The undersigned acknowledges that violation of the Stipulated Confidentiality Agreement may result in penalties for contempt of court.

Name:_____

Employer:_____

Business Address:_____

_____

Date:_____ Signature:_____

IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

RONDA COOPER, CORAL FRASER, DAVID GILTIN, and GILBERT MANDA, *on behalf of themselves and all others similarly situated,* Plaintiffs, v. MOUNT SINAI HEALTH SYSTEM, INC., Defendant.	No. 1:23-cv-09483 (PAE) Hon. Paul A. Engelmayer

STIPULATED ORDER GOVERNING
THE DISCOVERY OF ELECTRONICALLY STORED INFORMATION

1. PURPOSE

This Order will govern discovery of electronically stored information ("ESI") in this case as a supplement to the Federal Rules of Civil Procedure and any other applicable orders and rules.

2. COOPERATION

The parties are aware of the importance the Court places on cooperation and therefore they commit to cooperate in good faith throughout the matter consistent with this Court's guidelines and Individual Rules and Practices in Civil Cases.

3. PRESERVATION

To reduce the costs and burdens of preservation and to ensure proper ESI is preserved, the parties agree that:

a. They shall continue to take reasonable steps to preserve ESI relating to the above-captioned matter to the extent that it existed as of the date of the initiation of this putative class action lawsuit on October 27, 2023.

b. In terms of preservation, Defendant will continue to take reasonable steps to preserve relevant HTTP Archive format ("HAR") logs, Google Tag Manager container history and all other data sources in its possession, custody or control

demonstrating or evidencing the historical configurations of all tracking technologies at issue on Defendant's Website (https:// https://www.mountsinai.org/) and any databases to which those technologies could read or write data or metadata.

4. SEARCH AND IDENTIFICATION

The parties agree that in responding to an initial Federal Rule of Civil Procedure 34 request—or earlier if appropriate—they will meet and confer about methods to search ESI in order to identify ESI that is potentially subject to production in discovery and filter out ESI that is likely not subject to discovery. To limit the burdens and costs imposed by discovery in this matter, the parties shall use reasonable search methods to narrow down the ESI to be reviewed for production in discovery (*e.g.*, search terms, technology assisted review, de-duplication, elimination of correspondence with attorneys, client self-collection efforts, etc.).

The parties agree that the producing party is only required to produce a single copy of a responsive document or ESI and may remove exact duplicates across custodians as long as duplicate custodians are noted in production metadata.

5. PRODUCTION FORMATS

The parties agree to produce ESI in a format consistent with Appendix 1 of this Order.

6. PROPORTIONALITY

The parties agree that the proportionality standard set forth in Federal Rule of Civil Procedure 26(b)(1) must be applied in each case when formulating a discovery plan.

7. LIMITATIONS AND NON-WAIVER

The parties agree that this ESI Protocol is not intended to waive the rights to any protection or privilege including the attorney-client privilege, the work-product doctrine and/or any other privilege or immunity that may be applicable. The parties further agree that they are not waiving, and specifically reserve, the right to object to any discovery request on any appropriate grounds.

Further, nothing in this ESI Protocol shall be construed to affect the admissibility of documents and ESI. All objections to the discoverability or admissibility of any documents are preserved and may be asserted at any appropriate time. This ESI Protocol does not govern the appropriate scope of discovery under Rule 26(b)(1), and the specifics of custodian selection and search parameters or impose any obligations beyond those in the Federal Rules of Civil Procedure.

8. AUTHENTICITY AND ADMISSIBILITY

The parties have agreed that nothing in this ESI stipulation shall be construed to affect the authenticity or admissibility of any document or data. All objections to the authenticity or admissibility of any document or data are preserved and may be asserted at any time.

9. MODIFICATION BY AGREEMENT OR COURT ORDER

This Stipulated Order may be modified by a Stipulated Order of the parties or by the Court for good cause shown.

10. CONFIDENTIAL INFORMATION/CLAWBACK

The parties agree to seek any clawback of privileged material in a manner consistent with Appendix 2 of this Order

Date: December 10, 2024

Paul A. Engelmayer

UNITED STATES DISTRICT COURT JUDGE
PAUL A. ENGELMAYER

Agreed to by:

/s/ David A. Carney
David A. Carney (*pro hac vice*)
BAKER & HOSTETLER LLP
127 Public Square, Suite 2000
Cleveland, OH 44114
(216) 861-7634
dcarney@bakerlaw.com

/s/ James J. Bilsborrow
James J. Bilsborrow
WEITZ & LUXENBERG, PC
700 Broadway
New York, NY 10003
(202 558-5500
jbilsborrow@weitzlux.com

/s/ Robyn M. Feldstein
Robyn M. Feldstein
BAKER & HOSTETLER LLP
45 Rockefeller Plaza
New York, NY 10111
(212) 589-4201
rfeldstein@bakerlaw.com

Counsel for Defendant
Mount Sinai Health System, Inc.

/s/ David S. Almeida
David S. Almeida
ALMEIDA LAW GROUP LLC
849 W. Webster Avenue
Chicago, IL 60614
(312) 576-3024
david@almeidalawgroup.com

Counsel for Plaintiffs
and the Proposed Class

APPENDIX 1

PRODUCTION FORMATE AND METADATA

1. **Production Components** Except as otherwise provided in this Stipulation and Appendix, productions of hardcopy documents and ESI shall be in the following format: single page Group IV Tagged Image File Format ("TIFF") Images, searchable Text Files, an ASCII delimited searchable metadata file (.dat tile) and an image load file that can be loaded into commercially acceptable production software (e.g., CS Disco, Everlaw, Relativity).

2. **TIFFs** Documents and ESI should be produced as single-page TIFFs, imaged at a minimum of 300 dpi and produced in black and white or in color, so as to attempt reproduction of the hardcopy document. The document's original orientation should be maintained (i.e., portrait to portrait and landscape to landscape). Bates numbers, confidentiality designations and redactions (to the extent they are necessary) should be burned into the image. TIFF image files should be provided in "Images" folders, not to exceed 500 files per folder.

3. **OCR** Each hard copy document shall be run through optical character recognition ("OCR") software, and the full text shall be provided on a document-level in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. OCR shall be provided for all electronic documents as fully extracted text on a document-level in an appropriately formatted text file (.txt) that is named to match the first Bates number of the document. Text files should be provided in a "Text" folder. To the extent that a document is redacted, the text files should not contain the text of the redacted portions.

4. **Unique IDs** Each TIFF image should have a unique filename, which corresponds to the Bates number of that page. The filename should not contain any blank spaces and should be padded to 8 digits, taking into consideration the estimated number of pages to be produced. If a

Bates number or set of Bates numbers is skipped in a production, the producing party will so note in a cover letter or production log accompanying the production.

5. **Data Load Files** Documents and ESI should be provided with an Opticon Cross-Reference File and/or Concordance data load file using standard Concordance delimiters:

6. **Metadata** Paragraph 6 of this Appendix sets forth the minimum metadata fields that must be produced to the extent that metadata exists for a particular document or ESI. To the extent that metadata does not exist, is not reasonably accessible or available or would be unduly burdensome to collect, nothing in this ESI Protocol shall require any party to extract, capture, collect or produce such data except for those fields specially identified in Paragraph 6 immediately preceding the table in Paragraph 6.

Field Name	Field Description
BEGBATES	Beginning Bates number as stamped on the production image
ENDBATES	Ending Bates number as stamped on the production image
BEGATTACH	First production Bates number of the first document in a family
ENDATTACH	Last production Bates number of the last document in a family
HAS ATTACHMENTS	Indicates that an email has attachments
CUSTODIAN	The custodian of the document
PAGE COUNT	Total Number of pages in the document
OTHER_ CUSTODIAN	All individual(s) that had electronic files that were removed due to de-duplication (De-Duped Custodian) Field Name Field Description
DOCTYPE	The type of document (hardcopy) or electronic tile (e.g., Word, PDF, etc.) typically indicated by the file's extension
EXTENSION	Characters of the filename indicating the relevant portion used to open the file (file extension)

FULLPATH	The directory structure of the original file(s). Any container name is included in the path.
HASHVALUE	The MD5 or SHA-1 hash value
SUBJECT	Subject line of email
TITLE	Title from properties of document
DATESENT	Date email was sent (format: MM/DD/YYYY)
TIMESENT	Time email was sent
DATERECEIVED	Date email was received (format: MM/DD/YYYY)
TIMERECEIVED	Time email was received
PARENT_DATE	The date of the parent email should be applied to the parent email and all of the email attachments
TO	All recipients that were included on the "To" line of the email
FROM	The name and email address of the sender of the email
CC	All recipients that were included on the "CC" line of the email
BCC	Recipient(s) of "blind carbon copies" of the email message
AUTHOR	Any value populated in the Author field of the document properties
FILENAME	Filename of an electronic document
DATEMOD	Date an electronic document was last modified (format: MM/DD/YYYY)
DATECREATED	Date the document was created (format: MM/DD/YYYY)
NATIVELINK	Native File Link (Native Files only)
CONFIDENTIALITY	The document confidentiality designation, if any

7. **Text Files** A single multi-page text file shall be provided for each document or ESI and the filename should match the starting BEGBATES number of the document. A commercially acceptable technology for OCR shall be used for all scanned, hard copy documents. When possible, the text of native files should be extracted directly from the native file. Text files will not contain the redacted portions of the documents and OCR text files will be substituted instead of extracted text files for redacted documents.

8. **Redaction of Information** The producing party may redact from any TIFF image, metadata field or native file material that is protected from disclosure by applicable privilege or immunity or contains information subject to the terms of any agreed confidentiality order entered in this action. Each redaction shall be indicated clearly. If documents are produced containing redacted information, an electronic copy of the original, unredacted data shall be securely preserved in such a manner so as to preserve without modification, alteration or addition the content of such data including any metadata therein.

9. **Native Format** Electronic spreadsheets (e.g., Excel), electronic presentations (e.g., PowerPoint) or other file types that cannot be rendered into a static image and that have been identified as responsive and not privileged shall be produced in native format. The processed native for all such documents should be produced and linked to their corresponding documents by the metadata field "NATIVELINK." The requesting party may make reasonable requests for certain other electronic files and/or databases initially produced in their petrified (TIFF or PDF) format to be produced in their native format in the event that the petrified format is not reasonably usable. The requesting party shall identify the files or databases by their Bates numbers and the materials should be produced in their unaltered native format. To the extent that a native file must be redacted, the producing party may redact either the native file or produce TIFF images with burned

in redactions in lieu of a Native File and TIFF placeholder image. If redacting TIFF images and to the extent that any of the following can be automated, the producing party, or its e-discovery vendor, should make reasonable efforts to: (i) reveal hidden cells prior to converting the document to TIFF; (ii) clear any filters that may conceal information; (iii) adjust column widths so that numbers do not appear as "########"; (iv) ensure that column and row headings print and (v) ensure that the tab name appears in the header or footer of the document. If, however, the end user has not designated a tab name to appear in the header or footer of the document, no additional undertaking will be required by the producing party, including no custom handling or manual interventions.

10. **Relational Databases and Database Management Systems** The parties will meet and confer to attempt to agree upon the format of production by which discoverable ESI in a relational database or database management system (e.g., Oracle, Access, SQL server, 082) can be produced.

11. **Email and Attachments** Email and attachments should be converted to single-page TIFF images and produced consistent with the specifications provided herein. Attachments shall be processed as separate documents, and the text database load file shall include a field in which the producing party shall identify the email and the specific attachment or attachments to which that email is related.

12. **Word Processing Files** Word processing files, including without limitation Microsoft Word files (*.doc and *.docx), will be produced in the above TIFF format with tracked changes, comments and hidden text showing.

13. **Dynamic Fields** To the extent possible, files containing dynamic fields such as file names, dates and times will be produced showing the field code (e.g., "[FILENAME]" or

"[AUTODATE]"), rather than the values for such fields existing at the time the file is processed.

14. **Proprietary Files** To the extent a response to discovery requires production of ESI accessible only through proprietary software, the parties should continue to preserve each version of such information. The parties shall meet and confer to finalize the appropriate production format.

15. **Embedded Files** Except for signature blocks and non-substantive image files, embedded files must be treated as separate files. The load file shall include a field in which the producing party shall identify, for each document containing an embedded file, the production range of any such embedded file. This production range may be identified in the same field as the production range of an e-mail attachment.

16. **Compressed Files** Compressed file types (i.e., .CAB, .GZ, .TAR, .z, .ZIP) shall be decompressed in a reiterative manner to ensure that a zip within a zip is decompressed into the lowest possible compression resulting in individual files.

17. **Parent-Child Relationships** Parent-Child relationships (the association between an attachment and its parent Document) must be preserved in such a way that a document or electronic file and any attachments are produced in the same production set and the relationships identifiable. The parties agree to provide beginning attachment and ending attachment fields in the database load file to capture the entire production number range for the parent/child(ren) documents.

18. **Production Media Documents** shall be produced on external hard drives, readily accessible computer(s), FTP sites, email or other electronic media ("Production Media"). Each piece of Production Media shall identify a production number corresponding to the production volume (e.g., "VOL001," "VOL002"), as well as the volume of the material in that production

(e.g., "-001," "-002"). Each piece of Production Media shall also identify: (i) the producing party's name; (ii) the production date and (iii) the Bates number range of the materials contained on the Production Media. To maximize the security of information in transit, any media on which documents or electronic files are produced may be encrypted by the producing party. In such cases, the producing party shall transmit the encryption key or password to the requesting party, under separate cover, contemporaneously with sending the encrypted media.

19. **Processing Exceptions** The Parties agree that there is no need to preserve or collect ESI from the following sources, which are deemed to not likely contain relevant information and to be not reasonably accessible: deleted, fragmented or other data only accessible with the use of forensic tools; random access memory (RAM), temporary files or other ephemeral data that are difficult to preserve without disabling the operating system; online access data such as temporary internet files, history and cache; backup data that is substantially duplicative of data that are more accessible elsewhere; photograph files such as .jpg; server, system or network logs; data remaining from systems no longer in use that are unintelligible on the systems in use and any file with a logical size of zero.

20. **Unsearchable Documents** The Parties will make reasonable efforts to ensure that all ESI and document images are OCR-ed, all container files (such as PST or ZIP files) are successfully extracted and all encrypted or password-protected documents are successfully accessed, in order to ensure effective search, review and production under the requirements of this Stipulated Order. The Producing Party agrees to keep records of any files that are not successfully OCR-ed, extracted or accessed.

APPENDIX 2

CLAWBACK PROCEDURES

Any party who has received a privileged material notice from a producing party shall follow this procedure to ensure all copies of privileged material are appropriately returned, sequestered or destroyed from the receiving party's system:

i. locate each document in the document review/production database and return, sequester, or destroy the record from the database;

ii. if the document was produced in a write-protected format, the party seeking to recall the document shall, at its election, either (i) provide a replacement copy of the relevant production from which the document has been removed, in which case the receiving party shall destroy and render unusable the original production media; or (ii) allow the receiving party to retain the original production media, in which case the receiving party shall take steps to ensure that the recalled document will not be used and

iii. confirm that the recall of privileged material under this procedure is complete by way of letter to the Party seeking to recall privileged material.